



DATE : April 20, 2020

TO : Risk Management Contacts
(Please also Immediately Distribute to your respective System CEOs, General Counsels, CIOs, CISOs, CROs, COOs and Directors of HR)

FROM : FCC Services Risk Management Team

SUBJECT : Cyber Incident Reporting Guidelines

Dear System Risk Management contacts:

FCC Services, in conjunction with Aon our Cyber Insurance Broker, have successfully partnered with Beazley's Cyber Insurance Claims and Underwriting team to provide a streamlined and effective method for reporting Cyber incidents and receiving responsive communication during and after normal business hours, including weekends and holidays.

Cyber coverage is intended to provide both services and financial assistance to mitigate the impact of data breaches and cyberattacks. Some common examples of costs covered by the First Party section of the Cyber Policy include but are not limited to:

- Forensic services to investigate the existence of a breach
- Legal services to advise on your notification obligations
- Expenses incurred to communicating with affected customers
- Credit monitoring expenses
- Expenses to execute Public Relations and Reputation Management Campaigns
- Malicious destruction of data
- Denial of service attack
- Ransom negotiator services if your data is encrypted by malicious malware
- Virus, malware or spyware planted on your computer hard drive
- Call center services

The Third-Party Coverage section of the policy protects the System Institution for liability and legal expenses arising from employees and customers Personally Identifiable Information (PII) being compromised. These expenses are also covered.

Cyber Incident Response After Normal Business Hours Reporting Guidelines

The outline below highlights how Cyber incidents are to be reported and handled. As the circumstances of each Cyber incident are unique these guidelines may not address *every* scenario.

If a First Party Breach incident arises within your institution, or you receive a third-party complaint such as a lawsuit, please complete the following:

- Notify FCC Services and Beazley as soon as you suspect that personal or confidential information might have been compromised **and** once you have consulted with your Institution's General Counsel to maintain client/attorney privilege.
- Complete the Cyber claims form provided on FCC Services' website.
- Submit the Cyber claims form to fccs.claims@beazley.com **and** make sure to copy CyberClaims@fccservices.com in order to receive proper communication from all parties.
 - Please be sure to be as descriptive as possible in your email submission regarding the nature of the event as it will aid Beazley in prioritizing a timely response to your specific case.
- Within 24 hours, a Representative from the Beazley Breach Response ("BBR") Team will call to connect you with vendors and services to help minimize the exposure for urgent first party breaches and ransomware events. The BBR team monitors Beazley's claims inbox after normal business hours, on weekends and holidays and will reach out to you as quickly as possible. Third party claim submissions will be assigned to a Cyber claim manager with anticipated acknowledgment within 48 hours.
 - **Please note that the BBR Representative will not be able to offer a coverage opinion. The BBR Representative will coordinate a call with the Claim Manager assigned to the matter and FCC Services' claims team when appropriate.**
- Keep your General Counsel copied on all written communications.
- Beazley will provide a written coverage position once the claim has been assigned to a claim manager. The coverage summary typically occurs within 30 days.
- Please be sure to include FCC Services' claim representative on any and all communications with the BBR team, Beazley, and their vendors.

While this overview is not meant to be fully inclusive when reporting all claims, we hope that it provides the appropriate guidance as to what should be done in the event of a breach, ransomware attack or a lost or stolen electronic device resulting in personal identifiable information being compromised. Please note that the guidelines should not be construed as guaranteeing or representing coverage for future claims.

Please address you questions regarding these procedures to any one of the FCC Services' contacts included on the next page.

Cyber Incident Response After Normal Business Hours Reporting Guidelines

Chris Chappell - Claims Director

Tel: 303-721-3266

Email: Chris.Chappell@fccservices.com

Naomi Baumann - Professional Lines Examiner

Tel: 303-721-3263

Email: Naomi.Baumann@fccservices.com

Don Sicard - VP Risk Management

Tel: 303-721-3290

Email: Don.Sicard@fccservices.com

Lisa Parrinello - Insurance Director

Tel: 303-721-3214

Email: Lisa.Parrinello@fccservices.com